FOLEY
FOLEY & LARDNER LLP

ATTORNEYS AT LAW
777 EAST WISCONSIN AVENUE
MILWAUKEE, WI 53202-5306
414.271.2400 TEL
414.297.4900 FAX
WWW.FOLEY.COM

WRITER'S DIRECT LINE
414.297.5518
awronski@foley.com EMAIL

CLIENT/MATTER NUMBER
012474-0426

September 30, 2018

CONFIDENTIAL

Via Email

Charles J. Nerko
Vedder Price, P.C.
1633 Broadway, 31st Floor
New York, NY 10019

Re: *Bessemer System Federal Credit Union – Notice of Claims and Demand for Preservation of Documents*

Dear Charles:

Between September 24 and 26, 2018, Fiserv Solutions, LLC ("Fiserv") was subjected to a brute force attack on the servers and systems that perform Virtual Branch services for over 700 Fiserv clients, including Bessemer System Federal Credit Union ("Bessemer"), which you represent with respect to an unarticulated claim against Fiserv. Over three million attempts to authorize virtual banking transactions were made during this time. Fiserv identified that this activity was centered on accounts maintained on Fiserv's systems and belonging to Bessemer's customers. The servers and systems that were attacked are not dedicated to Bessemer and its customers and do not belong to Bessemer or its customers; rather, they belong to Fiserv. The size and scope of the attack strongly suggested to Fiserv that an unauthorized attempt to penetrate its clients' accounts was underway. Fiserv committed significant resources and successfully repelled the attack. Nonetheless, the attack caused a disruption of service, including, among other things, system latency and delays and the failure of certain processing transactions. That disruption, in turn, adversely impacted Fiserv and, notwithstanding the fact that there does not appear to have been unauthorized access to accounts or personal information, potentially its clients and consumers. Fiserv's investigation into the full scope and extent of these damages is continuing.

Upon identifying and discovering the attack, Fiserv immediately attempted to notify Bessemer. But Joy Peterson (Bessemer's CEO) refused to take calls from Fiserv and directed Fiserv to communicate with her by email. When Fiserv sent her a security update by email and clearly communicated that it was contacting her regarding an urgent security issue, Ms. Peterson still did not respond. Under the circumstances, this seemed highly unusual.

On September 28, 2018, I received a letter from you revealing that Bessemer initiated an event you characterized as a "security review" which, based on its timing and description in your letter, appears clearly to be the attack on Fiserv described above. We believe that explains Ms.

Peterson's evasion. Given that Bessemer would not communicate with Fiserv during the attack, it is apparent that much of the information and details in your letter must have come from a person that orchestrated or was materially involved in the attack. You have obviously communicated, directly or indirectly, with such individual(s) and have access to reports, transaction logs, or other physical or electronic records, wrongfully obtained, that will establish the nature and scope of the methods used in the attack, which you have not provided to Fiserv.

Assuming (as we do) that what your letter describes as a "security review" and the attack that Fiserv experienced are the same event; your description is wholly inapt. The " security review" was nothing of the sort. As you are well aware, Bessemer has notified Fiserv that it will not renew the Master Agreement and (presumably) is in the process of planning its deconversion and transition to another processing provider, which will occur in just a few short months. As you also know, Bessemer has filed an action against Fiserv and has failed to pay, and refuses to pay, invoices for processing and related services that Fiserv continues to provide. At best, your so-called "security review" was clearly a misguided, unauthorized attempt to manufacture some additional "issue" for Bessemer to use as leverage to escape its clear contractual obligations. Perhaps it was an aggressive – and wrongful – effort to obtain discovery for use in litigation against Fiserv. Indeed, it is not a coincidence that the attack followed shortly on the heels of my September 14, 2018 letter to you confirming Fiserv's intent to file counterclaims to compel Bessemer to pay the delinquent invoices it has refused to pay since July. No legitimate concerns about "security" could have motivated this attack; it was initiated by Bessemer with an improper motive, and executed through wholly improper means. Moreover, Fiserv's investigation strongly indicates that Bessemer intentionally skewed and tried to pre-ordain the results of its "security review" by providing assistance and information to those who executed the attack.

The attacker targeted servers and systems that belong to and are operated by Fiserv and serve hundreds of clients in addition to Bessemer. These servers and systems are not Bessemer's. Bessemer had no contractual right (and your letter certainly cites none) under the Master Agreement to interfere with Fiserv's systems. To the contrary, Bessemer's conduct clearly constitutes, at a minimum, a breach of Section 3 of the ASP Services Exhibit to the Master Agreement:

> 3. Fiserv System and Client Systems. Fiserv systems used in the delivery of Services (the "**Fiserv System**") and Client's networks and computer systems ("**Client Systems**") contain information and computer software that are proprietary and confidential information of the respective parties, their suppliers and licensors. ***Each Party agrees not to attempt to circumvent the devices employed by the other party to prevent unauthorized access thereto,*** including without limitations modifications, decompiling, disassembling, and reverse engineering thereof.

(emphasis added). Bessemer also clearly breached Section 5(g) of that same exhibit, which requires Bessemer to "notify Fiserv as soon as possible upon becoming aware of any incident of unauthorized access to any Information or the Fiserv System." Bessemer not only failed to notify Fiserv of the attack (of which it was obviously aware), but ignored Fiserv's attempts to communicate with Bessemer about that matter. As a result, Fiserv lacked information concerning the true nature and scope of the threat, causing Fiserv to incur additional damages and potentially putting Fiserv's other clients unnecessarily at risk. Further, Section 3(b) of the Master Agreement restricts Bessemer's use of Fiserv Information to "the lawful purposes contemplated in the Master Agreement"; the attack appears to have had no lawful purpose.

Your claim that the "security review" that Bessemer initiated was authorized by federal regulations[1] is wrong. The regulation you cited, and the surrounding authorities, do no more than charge a credit union with supervising and monitoring its third-party service providers. ***No regulator would sanction a surprise, sustained brute force attack on a third-party provider's servers that could potentially negatively affect hundreds of other financial institutions.*** It is no surprise, therefore, that a diligent review has revealed nothing authorizing Bessemer to invade and interfere with Fiserv's servers and systems through a "security review."

Nothing does. In fact, the opposite is true. Fiserv is actively investigating whether the conduct by Bessemer and the other third parties that planned, coordinated or executed it violates and gives rise to claims (both civil and criminal) under the Computer Fraud and Abuse Act, 18. U.S.C. § 1030, and similar state laws that prohibit unauthorized access to and penetration of computer systems, as well as common law claims for, among other things, conversion, trespass, and tortious interference.

This is a very serious matter. Fiserv is actively investigating and will pursue all available rights and remedies aggressively. In light of the seriousness of this matter, Fiserv demands that Bessemer immediately do the following:

1. Turn over to Fiserv the identity and contact information of all third parties who were involved in planning, executing or analyzing the "security review."

2. Turn over to Fiserv all reports, transaction logs, analyses or other records, whether physical or electronic, that relate to the "security review" in any way. **Fiserv hereby demands that Bessemer, its attorneys, agents, and any third party who was involved in, or has otherwise gained information regarding, the "security review" preserve and maintain all such records.**

[1] Specifically, your September 28, 2018 letter cites 12 C.F.R. Part 748, Appx. A § III.D.3.

FOLEY

FOLEY & LARDNER LLP

3. Refrain from dissemination or disclosure of any information or records relating to the "security review" to third parties, including any clients or competitors of Fiserv or media sources. All such information and records were improperly obtained, and any such dissemination or disclosure would be in furtherance of the misconduct against Fiserv. Given the nature of the misconduct, any reports or results generated constitute confidential Fiserv Information within the meaning of the Master Agreement.

If the "security review" your letter describes was something other than the attack, you should promptly provide a description of the scope and methods employed. If they are one in the same, Fiserv will not stand for such tactics, and will take all necessary and appropriate action to protect its rights and its clients.

We look forward to your prompt reply.

Very truly yours,

Andrew J. Wronski

Andrew J. Wronski

cc: Lynn S. McCreary
Amy L. Vandamme